Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Criteria for Evaluating Authentication Systems

Steven C. Way
McMaster University, steveway@mcmaster.ca

Yufei Yuan
McMaster University, yuanyuf@mcmaster.ca

Criteria for Evaluating Authentication Systems

Steven C. Way
DeGroote School of Business
McMaster University
steveway@mcmaster.ca

Yufei Yuan
DeGroote School of Business
McMaster University
yuanyuf@mcmaster.ca

ABSTRACT

User authentication is an important component of information security. It is critical in addressing many concerns that consumers and business have over the risk of identity theft. However, there is no systematic method to measure how good an authentication mechanism is in a given business context. This paper outlines nine criteria businesses can use to assess authentication systems. With these criteria, businesses are better equipped to select authentication systems that meet the needs of both their organization and their customers, and provide better protection against identity theft and other computer crimes.

Keywords

Authentication, evaluation criteria, information security.

INTRODUCTION

Information systems security is often defined as the confidentiality, integrity, and availability of an information system. Authentication is a key aspect of information systems security often associated with confidentiality (Tipton and Henry, 2007). Authentication is the verification of the unique identity of a user or system so that the user can gain certain privileges for system access and is the first step leading to the security constructs of accountability, auditing, and rights provisioning (Tipton and Henry, 2007).

Authentication may be verified by what an entity knows (knowledge), by what an entity owns (token), or by what an entity has in the form of a characteristic (Tipton and Henry, 2007) in order to control access to desired systems. Knowledge-based (KBA) and token-based authentication (TBA) are the two traditional techniques of authentication used (Jain, Hong, and Pankanti, 2000), although use of characteristic-based authentication (CBA) such as fingerprints, facial recognition, and other biometrics are on the rise. Table 1 provides a sample of several authentication applications with the typical mechanism listed.

Sample Application	Knowledge-based	Token-based	Characteristic-based
Credit purchase in store		Card	Signature
Credit purchase online	Card number		
ATM cash withdrawal	PIN number	Card	
Credit purchase at gas station		Card or RFID key	
Automobile membership services		Card	
Customs		Passport	Face
IS system user access	Password		
Secure VPN	Password	Digital token	
Security room	Password	Key	Iris/Retina scan
PDA/Laptop			Fingerprint

Table 1. Authentication Examples

Inappropriate or inadequate authentication may cause serious damage to systems and users. Criminals are highly motivated to circumvent access controls and gain access to systems to perform fraudulent and other illegal activities. Cyber crime and identity theft have caught consumers' attention where concerns over fraud are cited as a top reason for avoiding online shopping (Harvey, 2008). According to one survey of identity theft victims, 19% of known thefts were conducted online or via data breaches, and a further 23% were conducted during a transaction (Kim, 2008). Once an identity has been stolen it

may further be used to gain access to other systems and services. Therefore, strong authentication systems become a critical issue in combating identity theft and identifying fraud (Wang, Yuan, and Archer, 2006). As the first step for accessing a system, authentication is also an early line of defense against identity theft. The ability to measure and compare authentication systems would assist in determining the best methods of authentication for different systems. Aligning appropriate authentication mechanisms with information systems would reduce the risk of unauthorized system access. It will also help to relieve customers' concerns on security risks and boost their confidence.

Several papers have discussed authentication performance measurements for specific biometric authentication methods (Golfarelli, Maio, and Malton, 1997; Jain et al., 2000). Burrows et al. (1990) identified metrics of accuracy, speed, storage, cost, and ease of use, affect efficacy as being important for examining biometrics performance. In addition, they also pointed out that authentication data collection should be universal, unique, permanent, collectable, and consider performance, acceptability, and circumvention techniques. However, to the best of our knowledge, there is no general theoretical framework to address the evaluation criteria and performance measurement for a variety of authentication methods.

The purpose of this paper is to develop a comprehensive authentication assessment framework and to setup the criteria and performance measurement that can be used by both IT support and management personnel to evaluate an authentication system for business applications. The tool will incorporate criteria addressing not only technical, but also behavioral, and social issues. The authentication evaluation criteria and performance measurement can be used for developing and selecting the most appropriate authentication method for a variety of systems under a variety of situations. It will allow decision makers to make appropriate decisions impacting security, and authentication specifically, which may have long term influences on overall organizational performance.

A FRAMEWORK FOR PERFORMANCE EVALUATION CRITERIA

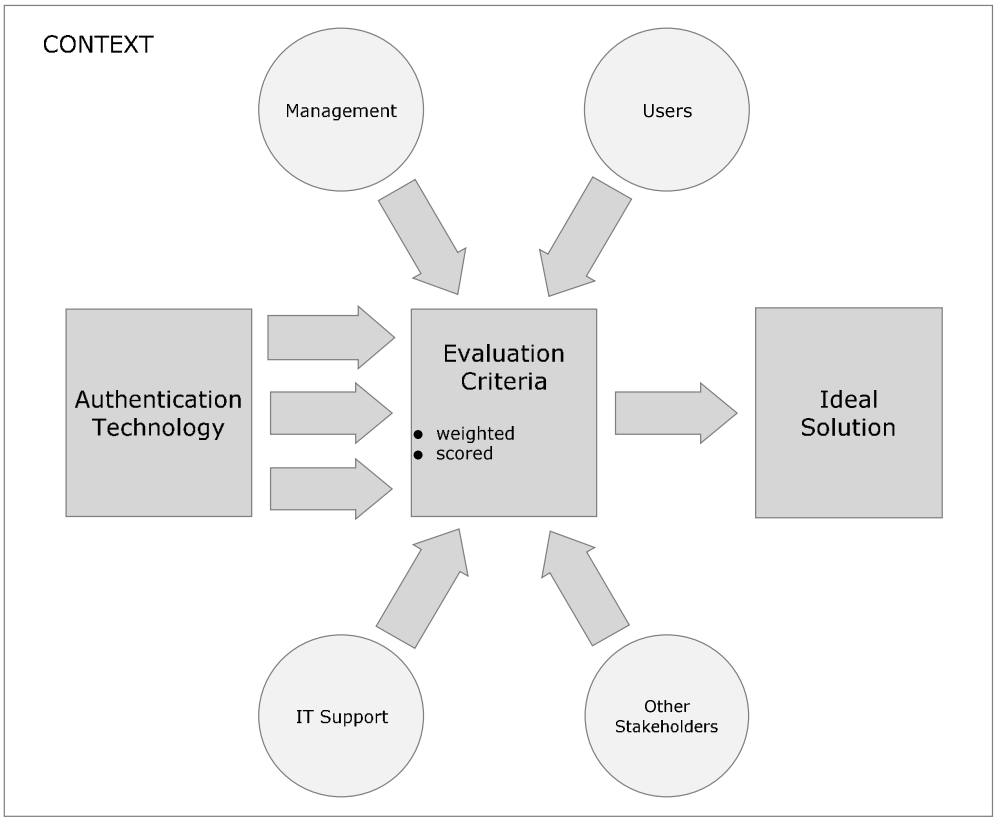

Figure 1. Decision Framework using Evaluation Criteria

We propose a framework as shown in Figure 1 to evaluate authentication technologies in order to determine the ideal solution for a given context. Several potential authentication technologies utilizing various authentication techniques are evaluated and compared to one another through the use of criteria established by key stakeholders. This study assumes the three most important stakeholders are organizational management, IT support personnel, and system users. Stakeholders are able to recommend various criteria according to their perspectives, making the framework comprehensive and able to address concerns from different stakeholders covering management, technical, and behavioral issues. Authentication technologies can then have their features scored based on the estimated value of the criteria from stakeholders and experts, and the scored criteria can further be modified by a weighting of criteria according to stakeholder priorities. The highest scoring authentication technology becomes the ideal solution.

This framework and methodology is consistent with the analytic hierarchy process (AHP) (Saaty, 2008). In AHP, the strength of the decision is based on the criteria selected and the criteria weighting from various stakeholders. Criteria are often weighted based on pair-wise comparison by the stakeholders performing the evaluation.

The criteria for the evaluation of authentication technologies have been selected based on literature and authors' previous professional experience. They are summarized in Table 2. These criteria affect the overall effectiveness and efficiency of an authentication mechanism. They are closely related to each other but each can be measured independently. On their own, each criterion must meet a minimum threshold set by an organization to determine acceptability, but together, the criteria can be used to compare different authentication techniques in a given context.

Criterion	**Definition**	**Supporting References**
Accuracy	- the capability of the authentication system to correctly determine a user's identity	(Bolle, Connell, and Ratha, 2002) (Golfarelli et al., 1997)
Robustness	- the capability of the authentication system to resist compromise	(Part I: Introduction and general model. 2006)
User Acceptance	- the willingness of users to use the authentication system	(Davis, 1989)
Accessibility	- the availability of the authentication system to target users	(Gong, 1993)
Feasibility	- the practicality of implementing the authentication system	(Sandhu, 2003)
Applicability	- the capability to apply the authentication system to different contexts by owners	(Chung-Huang Yang, 1999)
Responsiveness	- the speed of the authentication system to respond to users	(Menasce, 2003)
Non-reputability	- the capability of the authentication system to prevent a dispute with users about access to a system	(Gürgens, Rudolph, and Vogt, 2005)
Maintainability	- the effort required to maintain the integrity of the system	(Rombach, 1987)

Table 2. Authentication Evaluation Criteria

The importance of these criteria may be viewed differently by different stakeholders. Figure 2 clusters the criteria by hypothesized stakeholder priorities.

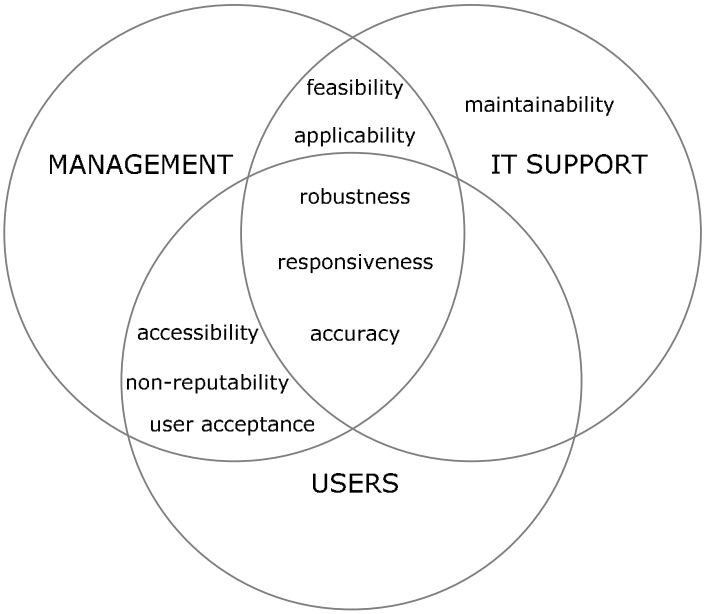

Figure 2. Stakeholder Perspectives on Authentication Criteria

The measurement of each evaluation criterion

Accuracy

Accuracy is a criterion that has multiple meanings as a metric. In the world of biometrics, accuracy may be referred to as the "degree of match" which is often characterized by false rejection and false acceptance error rates (Bolle et al., 2002). For authentication, however, it is necessary to have a more exact perspective for accuracy because a single user's identity is either accepted by a system, or it is rejected. A binary statistical classification from the world of multivariate statistics is a more appropriate perspective on accuracy. With this, there are four possible outcomes for user authentication to a system as follows: a correct user who is granted access (true positive), an incorrect user who is granted access (false positive), a correct user who is denied access (false negative), and an incorrect user who is denied access (true negative). Table 3 provides a summary.

EXPECTED OUTCOME vs. Actual Result	**TRUE**	**FALSE**
Positive	True Positive	False Positive
Negative	False Negative	True Negative

Table 3. Accuracy Results: Expected Outcome vs. Actual Result

The accuracy of a user authentication system can be defined as the correct determination of a user's identity. An accuracy rate is summarized mathematically as the number of correct determinations of a user's identity, both valid and invalid users, divided by the total number of authentication attempts.

$$AccuracyRate = \frac{(TruePositive + TrueNegative)}{(TruePositive + TrueNegative + FalseNegative + FalsePositive)}$$

Figure 3. Accuracy Rate

With token and KBA systems, accuracy is generally determined by the correct presence and check of the data required by the system. For biometrics systems, accuracy is measured by an error rate, i.e. the percentage of subjects being identified incorrectly (Bolle et al., 2002). There are two types of errors: type I errors where the correct subject is rejected, and type II errors where the incorrect subject is accepted (Jain et al., 2000).

The accuracy of authentication systems is dependent on the technology being used. With biometrics, problems related to pattern recognition errors are difficult to determine (Golfarelli et al., 1997). Noise in a sensed data signal such as dust on a fingerprint reader, or background noise on a voice recognition system may affect accuracy (Jain and Ross, 2004). Accuracy may also be affected by the coincidence of two similar patterns such as fingerprints, or the cross-over rate of type I and type II errors related to iris recognition (Golfarelli et al., 1997). Problems may also arise due to a change in a sensor (Jain and Ross, 2004) where two sensors may not read data in an identical fashion. While the examples above all reduce accuracy, an increased number of biometric dimensions being measured can help reduce cross-over errors resulting from false acceptance and false rejection errors (Golfarelli et al., 1997). In addition, using more than one biometric technique in the same system should also increase the accuracy of the system(Jain and Ross, 2004).

In order to properly use the assessment tool, the maximum acceptable error rates must be set by an organization. Tiers of acceptable accuracy levels should then be set to differentiate between various authentication techniques. Authentication techniques with error rates greater than the maximum acceptable rate can be excluded from further evaluation. Finally, the error rates for a given authentication technique should be either determined through theoretical calculations (Golfarelli et al., 1997) from a simulation, or sample testing if possible.

Robustness

Robustness is the ability to prevent or resist compromising attacks such as sharing, stealing, imitation, and counterfeiting. In KBA robustness is traditionally measured as how difficult it is to guess a password or the length of time the authentication mechanism can withstand direct brute-force attacks as determined by the encryption strength or the password length (Jain and Ross, 2004). In TBA, robustness can be measured by how difficult it is for a criminal to make a fake ID and the capability of the system to detect a fake ID card. The robustness of TBA can be improved by implementing some counterfeit technologies such as watermarks, holographs, hidden patterns, embedded IC chips, enhanced photos (Thompson, 2007), etc. Unlike KBA or TBA, biometric data is not easily stolen or shared (Jain and Ross, 2004). The robustness therefore should be measured by how difficult it is for a criminal to mimic a person's signature, voice, appearance, etc. (such as replicating the speed and movement when writing a signature, or matching more measured dimensions for facial features, etc.) and the capability of the system to detect the imitation.

Robustness would include the distinctiveness of data such as uniqueness of patterns (Jain and Ross, 2004). Other techniques to enhance robustness include resistance to spook attacks, multi-biometric systems, and challenge-response systems (Jain and Ross, 2004) or, the proper allocation of infrastructure resources to handle demand and system requirements, and alternative authentication techniques in the form of gradually strengthening authentication (Aura, Nikander, and Leiwo, 2001). Single, double, or triple authentication factors such as TBA only, TBA and KBA, or TBA, KBA, and CBA, will also greatly influence a method's robustness (Tipton and Henry, 2007). Lastly, any known vulnerabilities to an authentication mechanism should be considered.

With robustness being more technical in nature, measurement of an authentication technique on this criterion may be borrowed from the ITSEC standards on construction and operations vulnerabilities (*Information technology security evaluation criteria (ITSEC),* 1991) or the Common Criteria (Part I: Introduction and general model. 2006). Vulnerabilities analysis and knowledgeable security experts within the organization may assign a score to the authentication technique based on a robustness level determined from the ITSEC or Common Criteria scales.

User Acceptance

User acceptance is the willingness of users to use an authentication technology. Previous attempts to predict user acceptance relied on predicting the adoption rate of technology as indicated by perceived usefulness and ease of use by users (Davis, 1989). Where historical data is available, user acceptance can be measured by previous usage rates to predict the adoption rate of a new implementation. However, when new technology is to be deployed, surveys from technology acceptance models should be used to measure users' attitudes towards a technology as an indicator of users' willingness to use a new technology (Davis, 1989).

There may be a variety of user reasons for adopting a particular authentication technique. These benefits can include enhancing user convenience by eliminating passwords through the use of biometrics (Jain and Ross, 2004), or improving customer satisfaction through automation (Jain et al., 2000). Some authentication techniques may simply be mandated such as banks telling vendors they must start accepting smart credit and debit cards, and only issuing the new cards to consumers (Harvey, 2008). However, user acceptance may also be influenced by other issues such as the ease and comfort of acquiring data, and threats to privacy (Jain et al., 2000). User adoption may also be related to universality of data such that all users would need to possess a particular biometric attribute (Jain and Ross, 2004).

Accessibility

Accessibility is the availability of the authentication technology to users. Some may try to achieve accessibility through replication and distribution of the technology (Gong, 1993). Alternatively, accessibility may be the reduction of a dependence on a technology (Gong, 1993). Accessibility may be measured by the exposure of the authentication technology to the target audience. For example, banks and credit card companies in Canada are looking to add computer chips to their credit cards and debit cards in order to address fraud issues (Harvey, 2008). However, the implementation of a new technology such as this also requires that the hardware and readers must be available for vendors. Furthermore, even if there is a required widespread user-acceptance and adoption of the technology, vendors must still make the technology available for consumers to use in order for the authentication mechanism to be accessible, and therefore more effective overall.

Measurement of the accessibility of an authentication mechanism first depends on whether a closed environment such as in an organization or an open environment such as a restaurant is the location of use for the authentication mechanism. In the former case, 100% accessibility rate is presumed if an organization will ensure access to the mechanism. In an open system, however, accessibility should be determined from historical data, or projected data if a new authentication system is to be rolled out. An example of a rollout is the distribution of smart cards in Canada where 620,000 locations currently accept credit cards (Harvey, 2008). Accessibility is directly related to the proportion of locations that will have credit card readers able to accept the new smart-card technology.

Feasibility

Feasibility is the practicality of implementing an authentication technology. Feasibility is often associated with cost, but it may also be used to describe an organization's capability of implementing a system determined by the balance of features against other goals of the organization (Sandhu, 2003). Firms need to have the financial resources, the required operating environment, and the ability to meet organizational requirements. If a particular required element is lacking, then the difficulty of acquiring that element must be factored into the feasibility of the authentication mechanism. Generally, cost is the single most important factor for authentication security (Jain et al., 2000). Costs may be influenced by storage and processing requirements (Jain et al., 2000). The costs need to be balanced against risks associated with errors to determine an acceptable risk level (Jain et al., 2000). For multi-biometric systems, it is the balancing of cost versus performance which must be carefully considered (Jain and Ross, 2004), and for measuring authentication, this balance drives the measure for feasibility. Feasibility may also include other restrictions on a system such as capacity constraints.

Applicability

Applicability is the ability to apply an authentication mechanism to multiple scenarios. This aligns with other perspectives on applicability as the ability of a multi-purpose technology to be applied to multiple applications (Chung-Huang Yang, 1999). Applicability may be measured by determining the number of different applications a technology will be used for. For example, smart credit and debit cards may make sense for transactions done in-person, but smart card technology does not address online concerns so is not applicable to the context. In order to allow the use of smart cards for online transactions, consumers may require additional technology (Harvey, 2008). Similarly, some organizations may examine an ID card that can be used for physical security access in addition to systems access, while other organizations may employ ID cards for physical access, and use another technology such as passwords for online access.

Industry appears to be trying to improve the overall applicability of different authentication mechanisms. Many different systems appear to use similar requirements for accessing systems. This creates a scenario where access to many systems may be centralized and controlled by one user directory. In turn, a single sign-on process where a user only needs to sign-on once to a system may then be implemented. Once credentials have been successfully validated, users may then interact with several different applications. This process enhances authentication applicability as the shared common user credentials from

several one-to-one authentication to application relationships are merged to create a one-to-many authentication to applications relationship.

Responsiveness

Responsiveness is the performance of the system related to speed (Menasce, 2003). For users, speed is related to how quickly the system responds to an input, usually measured in a unit of time such as milliseconds. The responsiveness of a system influences the overall efficiency of an authentication system as it places restrictions on acceptable performance issues such as search times (Jain et al., 2000) which relate to data storage issues (Jain et al., 2000) and search algorithms used. For instance, a fingerprint search could be slow but the lookup could be much faster if the request was combined with a user ID as the user ID may be used as an index. Responsiveness also depends on the degree of automation. Automated data reading and verification can be much faster than manual data reading and checking. As system administrators configure authentication parameters to balance accuracy and costs, the overall responsiveness of the authentication technique considered will be influenced.

Non-Reputability

Non-repudiation has been defined as the inability for two parties to deny an exchange of data (Gürgens et al., 2005). For the purposes of authentication, non-reputability is the legally recognized ability of the system to prevent disputes for an exchange of data. Non-reputability examines aspects of an authentication mechanism that would track auditing of an authentication event in order to determine if it was successful or not and if the event involved the two known parties. Non-repudiation is particularly important when considering the impact on e-commerce or credit card fraud. Credit card transactions are based on the premise that the person providing the credit card number is the person named on the credit card and the account owner for the corresponding account at a financial institution. Non-repudiation means that a vendor and customer cannot dispute that a transaction has taken place. Similarly, non-repudiation means that a vendor and a financial institution cannot dispute that funds were transferred. In order to measure non-repudiation, parties to a transaction must use mutually agreed processes and technology to guarantee an exchange of data. For computer transactions, this often includes an exchange of public and private keys based on certificates for machines or accounts participating in a transaction. Deniability of a transaction may result in a loss of resources to an unknown source.

Maintainability

Maintainability is the amount of effort required to change a system or keep a system running properly over a period of time. As a metric, maintainability has been described as the average amount of effort required per maintenance task to support a technology (Rombach, 1987). Maintainability is a temporal measure and is often tracked in person-hours. When considering the maintainability of authentication mechanisms, one should examine the amount of effort required to correct an error, such as a pattern collision in a fingerprint reader, or the amount of effort required to update or upgrade a system, such as moving from a 4-digit pin to a 6-digit pin. In general, maintainability looks at the future viability of an authentication mechanism given various foreseen and unforeseen problems. The ability to rapidly address any problems with an authentication technology reduces the number of maintenance hours on a technology which in turn makes the security system more efficient.

THE COMPARISON OF DIFFERENT AUTHENTICATION MECHANISMS

In this section we use our evaluation criteria to compare KBA, TBA, and CBA mechanisms in order to demonstrate the value and applicability of our evaluation framework.

Accuracy of KBA and TBA is generally higher than CBA. Assuming a valid user is attempting authentication, KBA and TBA compare predefined indexes with authentication data which has a binary choice of either 100% match or mismatch. CBA, however, tends to have less accuracy. CBA accuracy is affected by the number of biometrics dimensions utilized. Type I or type II errors may occur from pattern collisions or improper readings of the characteristic making overall accuracy for CBA slightly lower than KBA or TBA.

In terms of robustness, KBA is the least robust, then TBA, and CBA is the most robust mechanism. KBA is susceptible to user sharing of authentication information as well as password steeling, brute-force and dictionary attacks, while TBA is susceptible to token sharing and forgery. A physical token restricts the likelihood of simultaneous authentication from two or more locations. In addition, security mechanisms are constantly being improved on tokens to monitor locations where they are used and to prevent forgery. This makes TBA more robust than KBA. It is extremely difficult to share or replicate characteristic-based patterns since most are biologically linked. CBA may be susceptible to spoofing and brute-force attacks,

but these are more difficult to perform because biometric patterns must be simulated in order to create a pattern collision. An increased number of measurement points, or multi-biometric authentication further reduces this opportunity for attack, and restricts access to the system that may otherwise be granted in a collision. As a result, CBA is considered the most robust of the techniques.

Anecdotal observation indicates less robust authentication tends to have a high user acceptance. For KBA, memorizing a password is not invasive and the authentication process is usually routine involving a keyboard or touch-pad. High user acceptance is expected for KBA while TBA is slightly less. TBA often has an initial administrative requirement to generate the token. For example, passport administrative requirements may include the submission of a birth certificate, driver's license, or other form of accepted identification. In addition, a physical token must be carried in order to be authenticated. Depending on the number of systems a user has access to, the number of tokens a user must maintain may be inconvenient. These hindrances to TBA are often balanced by a simple authentication process with no need to memorize a password. This makes TBA moderately accepted by users. CBA has the lowest user-acceptance and also has an administrative requirement of registration prior to use. Privacy concerns are a major factor that contribute to low user acceptance. In addition, the authentication process itself may be intrusive to users who disapprove of retina scans, fingerprint readers, or other types of scans and may offset any convenience gains.

KBA tends to be widely accessible, with TBA less, and CBA the least accessible. A combination of high user acceptance and lower infrastructure costs means KBA is often easier to establish and more widely available than other mechanisms. With TBA, organizations requiring the use of tokens generally ensure the ability to use them is available wherever authentication is required, but it may not always be in place. A requirement for specific hardware is often associated with TBA making it less accessible. Like TBA, organizations that require CBA systems attempt to ensure the ability to use them is available wherever authentication is required. These organizations are required to invest in more expensive technology that consistently reads and analyzes characteristic patterns in the same way. This technology combined with decreased user acceptance leads to reduced accessibility.

Feasibility for KBA is generally high, TBA is moderate, and CBA is lowest. KBA is well documented, widely used, and generally the cheapest type of authentication mechanism to implement. For data management, only small amounts of storage are required and authentication is quickly confirmed by simple lookups based on a user id as a key. TBA mechanisms are also well documented and use readily accessible technology such as computers, and scanners. They use marginally more amounts of storage compared to KBA. In addition, dependence on a token generally requires more resources to create tokens. The extra expense to operate makes TBA less feasible than KBA. CBA is the least feasible of all the authentication methods. It is usually more expensive to implement than TBA because much of the equipment is more specialized. For data management, the largest amounts of disk space are required to store complex patterns and more processing power is required to perform the calculations to compare patterns.

In terms of applicability, KBA systems tend to be highly applicable to a variety of scenarios. This is in contrast to TBA which is the least applicable authentication mechanism. TBA systems tend to utilize specialized data to enhance security, and specialized algorithms to access the data. Widespread use of a token for multiple applications reduces security overall as the ability to read and process data needs to be shared by several systems. In addition, the technology required to process the token also needs to be available at all locations. Therefore, token-based applicability is generally low. CBA systems have moderate applicability. Universal availability of a characteristic which cannot be shared enhances security which provides more opportunities to deploy CBA in high risk and high security settings. For systems requiring CBA, any technology requirements are generally available, thereby making applicability moderate for CBA.

For responsiveness, KBA and TBA are highly responsive since systems quickly look up known responses in a database and compare with an authentication attempt to determine the validity of the credentials provided. Responsiveness may be affected by the number of records stored in a system, but this is common to most if not all authentication mechanisms and can often be improved through various database management techniques. CBA is the least responsive mechanism. Data in the form of patterns is obtained from users often using scanners, and these patterns are then compared to other stored patterns. The complexity and subtle variation of patterns requires more processing than other authentication forms, which reduces system responsiveness for users.

Non-reputability is often missing from KBA techniques. The potential for high false positive and false negative errors in accuracy from shared or forgotten knowledge creates doubt and deniability for users. Despite security policies, the sharing of passwords or security knowledge continues affording users the ability to dispute an exchange of data. Furthermore, the manner in which passwords are managed by administrators and communicated to users may also make non-repudiation difficult as users may argue they are not the only people who have access to passwords. TBA techniques create a moderate mechanism for non-repudiation to occur. The presence of a token means that deniability becomes an argument over who had

possession of a token, as opposed to who used a token. CBA techniques have the best mechanism for non-repudiation. The extreme difficulty in sharing or reproducing a characteristic makes deniability very difficult. In addition, the potential for false positives and false negative errors in accuracy are reduced as more characteristic measures are introduced, further limiting the deniability of an authentication event.

The maintainability of KBA mechanisms is generally high. The standard use and operation of KBA has created several management tools depending on the technology, with many common management processes known by technology experts. TBA mechanisms are generally more difficult, therefore scoring low on maintainability. The creation of a token and the replacement of a token if one is lost or stolen is a multi-step process. In addition, revocation of tokens is difficult to manage, as inactive tokens must often be tracked in addition to valid tokens. These are the primary reasons why TBA has low maintainability. The maintainability of a CBA mechanism is generally moderate. After initial registration there are few processes required to maintain or track characteristics as they are a part of users. Revocation of CBA should be easy to manage centrally as only a user's access needs to be adjusted. The complex nature of CBA technology means collisions from similar patterns may be difficult to resolve but since they are infrequent, the overall maintainability of CBA is moderate.

Criterion	**Knowledge-based**	**Token-based**	**Characteristic-based**
Accuracy	HIGH	HIGH	MED
Robustness	LOW	MED	HIGH
User Acceptance	HIGH	MED	LOW
Accessibility	HIGH	MED	LOW
Feasibility	HIGH	MED	LOW
Applicability	HIGH	LOW	MED
Responsiveness	HIGH	HIGH	LOW
Non-reputability	LOW	MED	HIGH
Maintainability	HIGH	LOW	MED

Table 4. Comparison Summary of Authentication Mechanisms

Table 4 summarizes the nine authentication criteria and how the three authentication mechanisms compare for each. No single authentication mechanism scores high in all the criteria, therefore, stakeholder weighting becomes the differentiating factor for selecting an authentication technology. Furthermore, while this demonstration focuses on general authentication mechanisms, specific techniques should be compared as variance in technologies, even using the same mechanism, will create variance in the scoring of the criteria. One other observation from the table is that if no one mechanism scores high in all the criteria, perhaps a combination of different techniques becomes the best solution. With the combination of authentication techniques, one technology may complement another to overcome a weakness, or create a synergy in criteria to improve the score for the authentication system. Table 1 which lists sample applications demonstrates how combinations of authentication mechanisms may be utilized for an authentication system.

CONCLUSION

In this paper, we have proposed a multi-criteria evaluation framework to assess the quality of authentication mechanisms and we have demonstrated the usability of this evaluation framework. As businesses ponder existing authentication mechanisms, and new authentication mechanisms in the future, these criteria should help aid in the evaluation process so that appropriate authentication mechanisms are chosen for the right context. Sensitive contexts would ideally have more robust and accurate authentication mechanisms, while commerce contexts may focus more on non-reputability, and leisure contexts may emphasize system responsiveness and user acceptance. With properly selected authentication mechanisms for a system, it is expected that identity theft and other cyber crimes would be less of a concern for businesses and consumers.

ACKNOWLEDGMENTS

Funding for this research was provided from the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

1. Aura, T., Nikander, P., and Leiwo, J. (2001) DOS-resistant authentication with client puzzles, *Security protocols,* Springer Berlin / Heidelberg.
2. Bolle, R. M., Connell, J. H., and Ratha, N. K. (2002) Biometric perils and patches, *Pattern Recognition,* 35, 12, 2727-2738.
3. Burrows, M., Abadi, M., and Needham, R. (1990) A logic of authentication, *ACM Trans.Comput.Syst.,* 8, 1, 18-36.
4. Chung-Huang Yang. (1999) On the design of campus-wide multi-purpose smart card systems, *Security Technology, 1999. Proceedings. IEEE 33rd Annual 1999 International Carnahan Conference on,*465-468.
5. Davis, F. D. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly,* 13, 3, 319-340.
6. Golfarelli, M., Maio, D., and Malton, D. (1997) On the error-reject trade-off in biometric verification systems, *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* 19, 7, 786-796.
7. Gong, L. (1993) Increasing availability and security of an authentication service, *Selected Areas in Communications, IEEE Journal on,*11, 5, 657-662.
8. Gürgens, S., Rudolph, C., and Vogt, H. (2005) On the security of fair non-repudiation protocols, *International Journal of Information Security,* 4,4, 253-262.
9. Hamilton, S., and Chervany, N. L. (1981) Evaluating information system effectiveness -- part I: Comparing evaluation approaches, *MIS Quarterly,* 5, 3, 55-69.
10. Harvey, I. (2008) Plastic gets smart, *Globe and Mail,* Published June 28, 2008, Retrieved July 2, 2008 from <http://www.theglobeandmail.com/servlet/story/RTGAM.20080626.wgtchipcard28/BNStory/lifeFamily/>.
11. *Information technology security evaluation criteria (ITSEC)*(1991) Luxembourg: Office for Official Publications of the European Communities.
12. Jain, A. K., and Ross, A. (2004) Multibiometric systems, *Communications of the ACM,* 47, 1, 34-40.
13. Jain, A., Hong, L., and Pankanti, S. (2000) Biometric identification, *Communications of the ACM,* 43, 2, 90-98.
14. Kim, R. (2008). *2008 identity fraud survey report,* Javelin Strategy and Research.
15. Menasce, D. A. (2003) Security performance, *IEEE Internet Computing,* 7, 3, 84-87.
16. Part I: Introduction and general model. (2006) *Common criteria for information technology security evaluation,* Common Criteria Implementation Board.
17. Rombach, H. D. (1987) A controlled experiment on the impact of software structure on maintainability, *Software Engineering, IEEE Transactions on,*SE-13, 3, 344-354.
18. Sandhu, R. (2003) Good-enough security, *Internet Computing, IEEE,* 7, 1, 66-68.
19. Saaty, T. (2008) Decision making with the analytic hierarchy process, *International Journal of Services Sciences,* 1, 1, 83-98.
20. Shelly, G. B., Cashman, T. J., and Rosenblatt, H. J. (2007) Chapter 11 - systems operation, support, and security, *Systems analysis and design* (7th ed., pp. 510-515), Course Technology.
21. Tipton, H. F., and Henry, K. (Eds.). (2007) *Official (ISC)^2 guide to the CISSP CBK,* Boca Raton, FL: Auerbach Publications.
22. Thompson, Allan. (2007) 5-year passport renewal combats fraud, *Toronto Star*, Published May 10, 2007, Retrieved May 18, 2009 from <http://www.thestar.com/comment/columnists/article/212086>.
23. WenJie, W., Yufei, Y., and Archer, N. (2006) A contextual framework for combating identity theft, *Security and Privacy Magazine, IEEE,* 4, 2, 30-38.